Increasing The Level Of Protection Of Patients' Personal Data On Telemedicine Platforms

M.A. Tursunova,
Muhammad al-Khwarizmi Tashkent State Technical University, Master's Student
S.Sh. Muminova,
Muhammad al-Khwarizmi Tashkent State Technical University, Senior Lecturer

Abstract
This thesis provides a comprehensive analysis of data protection mechanisms in modern telemedicine platforms and identifies their main technical, legal, and human-factor vulnerabilities. As a solution to the identified problem, a holistic protection model based on the “Defense-in-Depth” concept is proposed. The proposed model integrates three main components: 1) advanced technical measures such as end-to-end encryption (E2EE) and blockchain; 2) regulatory and legal improvements, including the harmonization of HIPAA and GDPR standards and strengthening the ownership of patient data; 3) a human-factor-oriented approach, which involves continuous cybersecurity education and training for healthcare professionals and patients.
Keywords: Telemedicine, data security, privacy, HIPAA, GDPR, multilayered protection, blockchain, patient data, Defense in depth.
Annotatsiya
Ushbu tezisda zamonaviy telemeditsina platformalaridagi ma’lumotlarni himoya qilish mexanizmlari kompleks tahlil qilingan va ularning texnik, huquqiy va inson omiliga oid asosiy zaifliklari aniqlangan. Aniqlangan muammoning yechimi sifatida “Ko‘p qatlamli mudofaa” (Defense-in-Depth) konsepsiyasiga asoslangan yaxlit himoya modeli taklif etilgan. Taklif etilayotgan model uchta asosiy tarkibiy qismni integratsiyalashgan holda birlashtiradi: 1) yakuniy nuqtadan yakuniy nuqtaga shifrlash (E2EE) va blokcheyn kabi ilg‘or texnik choralar; 2) HIPAA va GDPR standartlarini uyg‘unlashtirish va bemorlarning ma’lumotlariga egalik huquqini kuchaytirishni o‘z ichiga olgan normativ-huquqiy takomillashtirish; 3) tibbiyot xodimlari va bemorlar uchun uzluksiz kiberxavfsizlik ta’limi va tayyorgarligini nazarda tutuvchi inson omiliga yo‘naltirilgan yondashuv.
Kalit so‘zlar: Telemeditsina, ma’lumotlar xavfsizligi, maxfiylik, HIPAA, GDPR, ko‘p qatlamli himoya, blokcheyn, bemor ma’lumotlari, Defense in depth.

So‘nggi o‘n yillikda telemeditsina tibbiy xizmat ko‘rsatish tizimining ajralmas bo‘g‘iniga aylanishi natijasida geografik masofalar ahamiyatini yo‘qotdi, tibbiy xizmat sifati yaxshilandi hamda sog‘liqni saqlash xarajatlarini kamaytirish imkoniyati yaratildi. Shu bilan birga, tibbiy yordamning raqamli muhitga ko‘chirilishi bemorlarning sog‘liq haqidagi maxfiy ma’lumotlarini yangi turdagi xavflarga - kiberhujumlar, ma’lumotlar sizib chiqishi va ularning noqonuniy ishlatilishiga - duchor qilmoqda. Bemorning salomatligiga oid ma’lumotlar moliyaviy yoki oddiy shaxsiy ma’lumotlardan farqli o‘laroq, oshkor etilganda jiddiy ijtimoiy, ruhiy hamda iqtisodiy zararlarni keltirib chiqarishi mumkin. Shu sababdan, telemeditsina tizimlarining barqaror va ishonchli rivojlanishi bemor shaxsiy ma’lumotlarini kompleks himoya qilish choralari bilan chambarchas bog‘liqdir.
Ushbu maqolaning maqsadi mavjud telemeditsina platformalaridagi xavfsizlik zaifliklarini tizimli tahlil qilish va ularni bartaraf etish uchun amaliy, ko‘p qatlamli himoya modelini taklif etishdir.

1. Telemeditsinada ma’lumotlar xavfsizligiga tahdidlar

Telemeditsina ekotizimi bemorlar, shifokorlar, platforma ishlab chiqaruvchilar, bulutli xizmat ko‘rsatuvchilar va uchinchi tomon integratsiyalaridan iborat bo‘lib, har bir elementi o‘ziga xos xavflarni keltirib chiqaradi.

Tahdidlarni quyidagi toifalarga bo‘lish mumkin (1-jadval):

1.Texnik tahdidlar:

– Zaif shifrlash. Ko‘pgina platformalar ma’lumotlarni faqat uzatish jarayonida shifrlaydi, serverda esa ular ochiq holda saqlanadi, bu serverga ruxsatsiz kirish imkoniyatini oshiradi;

– Xavfli integratsiyalar. Elektron tibbiy yozuvlar tizimi va to‘lov tizimlari bilan integratsiyani ta’minlovchi API lardagi zaifliklar keng ko‘lamli ma’lumot oqishiga olib kelishi mumkin;

– Eskirgan dasturiy ta’minot. Platforma va uning komponentlaridagi o‘z vaqtida yangilanmagan xavfsizlik tuzatishlari (patch) hujumlar uchun ochiq eshik bo‘lib xizmat qiladi.

2.Huquqiy va boshqaruv bilan bog‘liq tahdidlar:

– Normativ bo‘shliqlar. Ko‘plab mobil sog‘liq ilovalari, agar ular qamrovdagi tashkilotlar tomonidan boshqarilmasa, HIPAA kabi qonunlar doirasiga tushmay qoladi;

– Transchegaraviy ma’lumot oqimlari. Bemor va shifokor turli mamlakatlarda joylashganda, HIPAA va GDPR talablari to‘qnashishi mumkin, bu normativ muvofiqlikni murakkablashtiradi;

– Nazoratning sustligi. Boshqaruvchi organlar tez rivojlanayotgan telemeditsina bozoridagi barcha platformalarni samarali nazorat qilish uchun resurslar yetishmovchiligidan aziyat chekmoqda.

3.Inson omiliga oid tahdidlar:

– Past xabardorlik. Tibbiyot xodimlari va bemorlarning kiberxavfsizlik xavflari (masalan, fishing hujumlari yoki zaif parollardan foydalanish) haqidagi bilimining yetarli emasligi eng keng tarqalgan zaiflik hisoblanadi;

– Qulaylikka intilish. Ko‘p bosqichli autentifikatsiya kabi qo‘shimcha xavfsizlik choralarini foydalanuvchilar qiyin va vaqt talab qiluvchi deb hisoblashi, ularni chetlab o‘tishga olib keladi.

1-jadval. Telemeditsina platformalaridagi asosiy xavfsizlik tahdidlari.

Tahdid kategoriyasi	**Tahdid turi**	**Tavsifi**	**Oqibatlari**
Texnik tahdidlar	Zaif shifrlash	Ma’lumotlarning to‘liq (E2EE) shifrlanmasligi	Ma’lumotlarning o‘g‘irlanishi va manipulyatsiyasi
	Xavfli API integratsiyasi	Uchinchi tomon interfeyslaridagi zaifliklar	Keng ko‘lamli ma’lumot sizishi
	Eskirgan dasturiy ta’minot	O‘z vaqtida yangilanmagan xavfsizlik tuzatishlari	Ma’lum hujum turlariga ochiqlik
Huquqiy tahdidlar	Boshqarishdagi bo‘shliqlar	Turli mamlakatlardagi qonunlarning mos kelmasligi	Qonunbuzarlik va jarimalar
	Transchegaraviy ma’lumot oqimi	HIPAA va GDPR talablarining to‘qnashuvi	Muvofiqlashtirish qiyinliklari
	Nazorat sustligi	Boshqaruvchi organlarning resurslari yetishmovchiligi	Qonunbuzarliklarning aniqlanmasligi
Inson omili tahdidlari	Fishing hujumlari	Xodimlarning firibgarlik xatlariqa tushib qolishi	Login ma’lumotlarining o‘g‘irlanishi
	Zaif parollar	Oddiy va takrorlanuvchi parollardan foydalanish	Ruxsatsiz kirish imkoniyati
	Xabardorlik yetishmasligi	Xavfsizlik protokollarini bilmaslik	Noto‘g‘ri ma’lumot boshqaruvi

Taklif etilayotgan ko‘p qatlamli himoya modeli

Mazkur muammolarni hal qilish uchun “bir qatlamga ishonmaslik” prinsipiga asoslangan “Defense in depth” modeli taklif etiladi. Ushbu model to‘rtta o‘zaro bog‘langan qatlamni o‘z ichiga oladi (2-jadval).

2-jadval. Ko‘p qatlamli himoya modelining tarkibiy qismlari.

Qatlam	Asosiy komponentlar	Amalga oshirish usullari	Kutilayotgan natija
Texnik asos	- End-to-End shifrlash (E2EE) -Ko‘p bosqichli autentifikatsiya (MFA) - Muntazam Audit	-Kuchli kriptografik algoritmlar -Biometrik autentifikatsiya -Tashqi ekspertlar tekshiruvi	Ma’lumotlarning maxfiyligi va yaxlitligini ta’minlash
Innovatsion texnologiyalar	- Blokcheyn - Zero Trust arxitekturasi - Sun’iy Intellekt	- O‘zgarmas audit izlari - Doimiy tekshiruv -Anomaliyalarni aniqlash	Proaktiv himoya va shaffoflik
Huquqiy mexanizmlar	- Global standartlarni uyg‘unlashtirish - Privacy by Design - Bemor huquqlari	- Xalqaro hamkorlik -Dizayn bosqichidagi integratsiya - Rozilik boshqaruvi	Qonuniy muvofiqlik va ishonch
Inson omili boshqaruvi	- Xodimlarni o‘qitish -Bemorlarni xabardor qilish -Foydalanish qulayligi	- Muntazam treninglar -Oddiy qo‘llanmalar - tushunarli interfeys	Xavfsiz xulq-atvor va mas’uliyat

1-qatlam. Asosiy texnik himoya choralari. Bu qatlam platformaning minimal xavfsizlik standartlarini belgilaydi:

– Yakuniy nuqtadan yakuniy nuqtaga shifrlash (E2EE). Barcha muloqot (video, audio, matn) va saqlanadigan ma’lumotlar butun yo‘lda shifrlangan bo‘lishi kerak;

– Kuchli autentifikatsiya. Parol bilan cheklanmasdan, majburiy ko‘p bosqichli autentifikatsiya (MFA) joriy etilishi lozim;

– Muntazam audit va sinovlar. Tashqi mutaxassislar tomonidan tekshiruvlar va suqilib kirishga testlash o‘tkazib turilishi zarur.

2-qatlam. Rivojlangan texnologik innovatsiyalar:

– Blokcheyn texnologiyasi. Ma’lumotlarga kirish va o‘zgartirish bo‘yicha o‘zgarmas audit izi yaratish, shuningdek, bemorning o‘z ma’lumotlari ustidan nazoratini ta’minlovchi aqlli shartnomalar (smart contracts) orqali rozilikni boshqarish;

– Zero Trust arxitekturasi. “Hech qachon ishonma, har doim tekshir” prinsipiga asoslanib, tarmoq chegarasidan qat’iy nazar, har bir so‘rov qat’iy tekshiruvdan o‘tkazilishi kerak.

3-qatlam. Huquqiy va siyosiy takomillashtirish:

– Global standartlarni uyg‘unlashtirish. HIPAA, GDPR va boshqa muhim qonunlarni telemeditsina kontekstida uyg‘unlashtirish;

– “Loyihalash jarayonidagi mahfiylik” (Privacy by Design) tamoyilini majburiy qilish. Platforma ishlab chiqilishining dastlabki bosqichlaridan boshlab maxfiylik va xavfsizlik talablari asosiy mezon bo‘lishi kerak.

– Bemorlarning ma’lumotlarga egalik huquqini ta’minlash. Bemorlar o‘z ma’lumotlarini kim, qachon va qanday maqsadda ishlatayotganini aniq ko‘ra olishi va boshqarishi lozim.

4-qatlam. Inson omiliga yo‘naltirilgan ta’lim:

– Xodimlarni muntazam tayyorlash. Tibbiyot xodimlari uchun real ssenariylar asosida phishing, ijtimoiy muhandislik va ma’lumotlarni noto‘g‘ri boshqarish xavflari bo‘yicha treninglar o‘tkazish;

– Bemorlarni bilimini oshirish. Bemorlar uchun maxfiylik siyosatlarini oddiy tilda tushuntirish va ularni o‘z ma’lumotlari xavfsizligi uchun mas’uliyatli harakatlar qilishga undovchi resurslar yaratish.

Quyida ko‘rib chiqilgan tahdidlarga qarshi yechim sifatida taklif etilgan choralar ta’sir doirasi bo‘yicha mosligi keltirilgan. 3-jadval turli xil tahdid turlari uchun qisqa muddatli, o‘rta muddatli va uzoq muddatli himoya choralari qanday moslashtirilishini ko‘rsatadi.

3-jadval. Tahdidlar va ularga qarshi himoya choralari mosligi.

Tahdid turi	**Qisqa muddatli chora**	**O‘rta muddatli chora**	**Uzoq muddatli chora**
Zaif shifrlash	TLS/SSL ni yangilash	E2EE ni joriy etish	Kuchli kalit boshqaruvi tizimi
Phishing hujumlari	Xodimlarni ogohlantirish	Muntazam treninglar	AI asosida filtrlash
Huquqiy tafovutlar	Mavjud qonunlar tahlili	Xalqaro standartlarga moslash	Global regulyator bilan hamkorlik
API zaifliklari	Mavjud API larni tekshirish	Xavfsiz kodlash standartlari	Avtomatlashtirilgan xavfsizlikka testlash

Xulosa

Taklif etilgan ko‘p qatlamli himoya modeli telemeditsina tizimlarida ma’lumotlar xavfsizligini ta’minlash bilan bog‘liq murakkab muammolarga kompleks yechim taklif etadi. Ushbu yondashuv faqat texnik himoya choralariga tayanib qolmay, balki huquqiy talablar va inson omilini bir butun tizim sifatida integratsiyalashni nazarda tutadi. Modelning ustunligi uning qatlamlararo o‘zaro ta’sirida namoyon bo‘ladi: bir qatlamdagi zaifliklar boshqa qatlamlar tomonidan kompensatsiya qilinadi va natijada barqaror, moslashuvchan hamda ishonchli himoya muhiti shakllanadi.

Amalda qo‘llash jarayonida esa bir qator cheklovlar mavjud — xususan, kichik telemeditsina platformalari uchun joriy etish xarajatlarining yuqoriligi, xavfsizlik va qulaylik o‘rtasidagi muvozanatni topishdagi murakkablik, hamda tizimni kengaytirishda zarur resurslarning yetishmasligi. Shu bilan birga, Sun’iy intellekt (AI) va Tibbiyot Interneti (IoMT) texnologiyalarining tez sur’atlar bilan rivojlanishi ma’lumotlar xavfsizligiga qo‘yiladigan talablarni yanada kuchaytirmoqda.

Xulosa qilib aytganda, telemeditsina platformalarida axborot xavfsizligini ta’minlash faqat texnik vazifa emas, balki bemorlarning ishonchini mustahkamlash va sog‘liqni saqlash tizimining barqaror rivojlanishini ta’minlash uchun muhim shartdir. Taklif etilgan ko‘p qatlamli yondashuv esa bu maqsadga erishishda amaliy, tizimli va strategik asos sifatida xizmat qilishi mumkin.

Adabiyotlar ro‘yxati:

Kruse, C. S., et al. (2017). Security techniques for the electronic health records. Journal of Medical Systems, 41(8), 127.

European Union Agency for Cybersecurity (ENISA). (2021). Data Protection in the Health Sector.

U.S. Department of Health & Human Services. (2020). HIPAA for Professionals.

Zhang, R., & Liu, L. (2020). Security models and requirements for healthcare cloud computing. IEEE Transactions on Cloud Computing.

Avancha, S., et al. (2012). Privacy in mobile technology for personal healthcare. ACM Computing Surveys.

Д.М. Монаков, В.А.Шадеркина, С.А.Рева, А.А.Грицкевич. Защита персональных данных пациентов при использовании телемедицинских технологий в период пандемии COVID-19. https://doi.org/10.29188/2712-9217-2021-7-4-48-57.